Amendments to the Claims

1.-3. (Cancelled)

4. (Currently amended) In a plural block cipher device, cryptographically secured digital communication system having at least a first ~~one~~ block cipher device that is computationally a function of ~~responsive to~~ a first fixed length selectively variable key to encrypt and decrypt a digital signal, and at least a second ~~one~~ block cipher device that is computationally a function of ~~responsive to~~ a second fixed length selectively variable key different from the first fixed length selectively variable key to encrypt and decrypt a digital signal, a ~~the~~ method of adapting a block cipher device having the first key for operation with a block cipher device having the second key the method comprising the step of effectively inhibiting the operation of the most downstream of ~~the~~ modulo operators in the block cipher device having the first key.

5. (Original) The method of Claim 4 wherein the effective inhibiting is accomplished by the step of modifying the key of the first block cipher device to conform to two sequential iterations of the key of the second block cipher device.

6. (Currently amended) In a cryptographically secured digital communication system, a method of selectively adapting a plurality of block cipher devices ~~device~~ having at least a first ~~one~~ block cipher device that is computationally a function of ~~responsive to~~ a first fixed length selectively variable key to encrypt and decrypt a digital signal for operation with a second block cipher device that is computationally a function of ~~responsive to~~ a second fixed length selectively variable key ~~fixed length~~ one half the length of the first key to encrypt and decrypt the digital signal the method

comprising the steps of:

(a) providing a first key generator having ~~in~~ two equal sections of symbols, each section a functional replica of a ~~the~~ second key generator;

(b) replicating the second key in both of sections of the first key;

(c) using the symbols provided by one of the two sections to encode and decode the signal in a first stage; and

(d) combining the symbols provided by the two sections of the first key generator to cancel the symbols applied to a second stage.

7. (Currently Amended) A block cipher device for encrypting and decrypting information in a cryptographically secured digital communication system comprising:

a key scheduler unit that is computationally a function of ~~responsive to~~ a key data block comprising:

a first function unit that is computationally a function of ~~responsive to~~ a first portion of the key data block for producing a first key data sub-block; and

a second function unit that is computationally a function of ~~responsive to~~ a second portion of the key data block for producing a second key data sub-block; and

an encryption stage that is computationally a function of ~~responsive to~~ the first and second key data sub-blocks where the encryption stage will not encrypt data if the first portion of the key data block is equal to the second portion of the key data block, and the first function unit is equal to the second function unit.

8. (Currently Amended) In a block cipher device used ~~use~~ in encrypting and decrypting information in a cryptographically secured digital communication system having plural encryption stages that are computationally a function of ~~responsive to~~ an input data block, a control data block, a key data sub-block, and a key scheduler for randomizing the key data sub-block, the improvement wherein the key scheduler comprises:

a first shift register;

a first means for randomizing a portion of the key data block using the ~~responsive to~~ said first shift register;

a first modulo two summing combiner for serially combining a serial output from the first shift register and the serial output from said first randomizing means to provide a first combined data output;

a first key data sub-block derived from the contents of said first shift register;

a second shift register;

a second means for randomizing a portion of the key data block using the ~~responsive to~~ said second shift register;

a second modulo two summing combiner for serially combining the serial output from the second shift register and the serial output from said second randomizing means to provide a second combined data output;

a second key data sub-block derived from the contents of the second shift register;

a third modulo two summing combiner for combining said first key data sub-

block and said second key data sub-block to produce a third key data sub-block;

a first function unit that is computationally a function of ~~responsive to~~ the second key data sub-block for providing a fourth key data sub-block; and

circuit means for providing said first, third and fourth key data sub-blocks to different ones of said plural encryption stages.

9. (Original) The block cipher device of Claim 8 wherein both said first and second randomizing means includes a selectively customized look-up table.

10. (Currently Amended) The block cipher device of Claim 9 [[11]] wherein the customized look-up table of said first and second means for randomizing are identical.